CENTRAL WEST | Credit Union
Your local banking partner

TIPS for STAYING SAFE ONLINE

- **Social Media Shopping**

Use caution when shopping from ads on Social Media. The concerns are that the ads are not legitimate and are scammers, that the quality of the product is not what it should be. (eg you think you have purchased a shirt from a Facebook ad but the debit to your account is from a Fitness site (*real life example*))

- **OTP (One Time Password)**

Consider these a life line to protecting your personal information. Giving out a OTP authorises scammers to transact on your Visa Card or gain access to sites such as your banking or MyGov accounts (real life experience). Transactions processed on your Visa card where a OTP has been provided cannot be disputed.

Never give out a OTP

- **Do Not Save Banking Passwords**

Whilst convenient, if you save a password to your device and allow remote access by a scammer to that device, they can log in to any account where you save your username and password. This could result in funds being transferred out of your banking accounts and is incredibly hard to recover.

- **Do Not Download Remote Access Apps**

Doing so allows scammers access to your devices – they can then change passwords to your emails, banking accounts and any other apps you use that requires a password. They can also transfer funds from your banking account and redirect payments from sites such as MyGov (*real life example*)

- **Do You Research Before Shopping**

Consider things such as; How can you contact the site, check the contact us page for email, phone number and address; What is the sites Refund and Returns Policy; Check the sites Terms and Conditions to ensure you are not signing up to any regular accounts; is the site Australian or Other, if other consider the exchange rate, cost of delivery and additional delivery time, check the site in general for poor use of language, spelling errors, low quality pictures.

- **Is the Price too good to be True?**

If it is, then chances are the site you are on is a scam site, mirroring a legitimate site. Check the contact page (eg if the site is Country Road and the contact us page has an email of rose@gmail.com it is not a legitimate Country Road site (*real life example*))

- **Use Caution when shopping from a Promoted/Sponsored site**

The site could be a phishing site by a scammer. Scammers can pay to have their phishing sites promoted/sponsored. See above Do your Research before Shopping.

-

- **Use Caution Responding to SMS/Emails asking to update Visa Card details**

These are typically scammers. If you provide your card details, any resultant transaction may not be able to be disputed.

- **Use Caution Responding to Surveys**

Whilst companies legitimately seek feedback, they will not offer the chance at the end of the survey to get an item for postage only (*real life example*).

- **Use Caution when signing up to Free Trials**

If you do not cancel the trial within the designated time frame, then it will convert to a regular subscription account. Any resultant transaction may not be able to be disputed.

What You Can Do

- **Trust Your Credit Union.**

Scammers may tell you not to trust your bank, scammers will tell you what to say to your bank so that they get the result they want (access to your account and/or card)
CWCU and its staff are there to help you, talk to us and provide any and all the information you can so we can help keep your account secure.

- **Call Vigil**

CWCU has a designated fraud monitoring company called Vigil. If you are experiencing problems with your card or you have given out your card details and are concerned, you can contact Vigil on 1300 705 750 or from overseas on 612 8299 9534

- **CWCU App/Internet Banking**

If you shop online, you should be regularly checking your bank account to keep an eye on your transactions.
You are the best person to monitor your account.
Our CWCU app has the added benefit of allowing you to block your card if you notice it as lost/stolen/missing or you have identified an unknown transaction on your card. Blocking the card will prevent any further activity until you can contact us or Vigil.

- **Consider Using PayPal**

PayPal keeps your financial information private and uses encryption to process transactions. PayPal's Purchase Protection program may apply when you encounter specific problems with a transaction

- **Secure Your Details**

If you have provided personal identification details, you can get further assistance from the following sites;
IDCARE - Australia and New Zealand's national identity & cyber support service. Visit their website https://www.idcare.org/ or call them on 1800 595 160
Clear Score – an app that can be downloaded and will provide free of cost your credit score and report.
It is important to act quickly and provide all details of what personal information and passwords were provided along with any apps that were downloaded to devices to CWCU so we can guide you effectively as to any further action to take.